We claim:

1. A computer system for detecting and monitoring network intrusion events from log data received from network service devices in a computer network, the computer system having discrete modules associated with a function performed on the log data received, the computer system comprising:

an event parser in communication with at least one network service device, the event parser being able to receive log data in real time from the device, the log data including information detailing a network intrusion event received from the network service device if an intrusion has occurred, the event parser being able to parse the information to create a corresponding event object concerning the intrusion event;

an event manager in communication with the event parser, the event manager being able to receive the event object, the event manager being configured to evaluate the event object according to at least one predetermined threshold condition such that, when the event object satisfies the predetermined threshold condition, the event manager designates the event object to be broadcast in real time;

an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event object in real time as an intrusion alarm; and

means for alerting the user that a network intrusion event has occurred.

2. The computer system of claim 1 wherein the means for alerting the user that a network intrusion event has occurred is a graphical user interface in communication with the event broadcaster, the graphical user interface comprising a display screen for displaying an intrusion

alarm and the information contained within the corresponding event object received from the event broadcaster.

3. The computer system of claim 2 wherein the graphic user interface is configured to allow a user to initiate queries, and the computer system further comprises:

means for storing event objects, said means coupled to the event parsers;

a report servlet coupled to the graphic user interface, the report servlet for recalling stored event objects in response to user queries from the graphic user interface and displaying recalled event objects on the graphic user interface display screen;

an application reporter coupled to the report servlet for receiving and processing user queries and for performing searches of stored event objects;

a database accessible by the application reporter, for holding stored event objects, the database configured to recall event objects in response to searches executed by the application reporter.

4. The computer system of claim 1 further comprising:

a network port to receive log data having a conforming message format from at least one network service device;

means for transmitting the log data having a conforming message format to the event parsers, said means coupled to the network port;

a reporting agent coupled to the network port for collecting log data having a non-conforming message format from the at least one network service device and converting the log data to a conforming message format.

5. The computer system of claim 4 wherein the conforming message format is syslog.

6. The computer system of claim 2 wherein the graphical user interface display screen comprises an alarm console, coupled to the event broadcaster, configured to display intrusion alarms, and a report console, coupled to the report servlet, configured to execute queries input by a user and display results, wherein the alarm console and event broadcaster are displayed simultaneously on the display screen.

7. The computer system of claim 6 wherein the report console is further configured to display query result data in summary lines, said summary lines comprising hypertext links providing access to further data.

8. The computer system of claim 6 wherein the alarm console displays intrusion alarms in summary lines, said summary lines comprising hypertext links providing access to further data.

9. The computer system of claim 6 wherein the graphical user interface displays the status of network security devices in real time.

10. The computer system of claim 9 wherein the graphical user interface displays the status of network security devices in summary lines, said summary lines comprising hypertext links providing access to further data.

11. The computer system of claim 10 wherein the graphical user interface displays the status of network security devices in a color coded format where said color designates a particular status level for the particular device.

12. The computer system of claim 6 further comprising a chat manager accessible to a user from the alarm console for executing electronic communications links between the user and others having an electronic communications link to the computer system.

13. The computer system of claim 12 wherein the electronic communications link is an on-line link established through a web browser interface.

14. The computer system of claim 1 further comprising a plurality of event parsers wherein each event parser is configured to receive log data from a predetermined network service device, the plurality of parsers each coupled to the event manager.

15. The computer system of claim 1 wherein the information contained within the event object is read by the event manager and assigned a severity level corresponding to the event type information contained within the event object, and the predetermined threshold condition is the assigned severity level.

16. The computer system of claim 1 wherein the severity level is one of seven categories for types of events contained within event objects.

17. The computer system of claim 1 further comprising an event aggregator module and wherein the event parser is housed within the event aggregator module, and log data from a multiplicity of network device sources is received by the event parser.

18. The computer system of claim 17 wherein the event parser reads log data posted in extensible markup language.

19. The computer system of claim 2 wherein the computer system is one of a multiplicity of computer systems each having a graphic user interface and the computer system further comprises a central graphic user interface which accesses at least one of the graphic user interfaces of the multiplicity of computer systems.

20. The computer system of claim 19 wherein the central graphic user interface accesses at least one of the report servlets of the multiplicity of computer systems and communicates with at least one of the databases of the multiplicity of computer systems.

21. The computer system of claim 1 further comprising means for filtering event objects received by the event manager according to one or more predetermined conditions so as to restrict the field of event objects designated for broadcast.

22. The computer system of claim 4 further comprising means for filtering log data received at the network port according to one or more predetermined conditions so as to restrict receipt of corresponding log data by said transmitting means.

23. The computer system of claim 21 wherein the predetermined conditions are application name, host name, event severity, internal device alarm identifications, source address, destination address, destination port, and protocol.

24. The computer system of claim 22 wherein the predetermined conditions are application name, host name, internal device alarm identifications, source address, destination address, destination port, and protocol.

25. A method for detecting and monitoring network intrusion events from log data received from network service devices in a computer network, comprising the steps of:

receiving log data in real time, the log data including information detailing at least one network intrusion event received from the at least one network service device;

parsing the log data information to create a corresponding event object;

evaluating the event object according to at least one predetermined threshold condition;

where the information contained within the event object satisfies the predetermined threshold condition, broadcasting the event object as an intrusion alarm in real time to a display screen on a graphic user interface.

26. The method of claim 25 wherein the graphic user interface is configured to allow a user to initiate queries, and the method further comprises the steps of:

storing event objects to a database accessible by an application reporter, the database for holding stored event objects, and the database configured to recall event objects in response to searches performed by the application reporter in response to user queries;

recalling stored event objects in response to user queries from the graphic user interface and displaying recalled event objects on the graphic user interface display screen;

27. The method of claim 26 further comprising the steps of:

receving log data in a conforming message format at a network port;

transmitting the log data in a conforming message format to event parsers;

collecting log data in a non-conforming message format by executing a reporting agent;

converting the log data to a conforming message format.

28. The method of claim 27 wherein the conforming message format is syslog.

29. The method of claim 25 wherein the event object intrusion alarm is displayed as a hypertext link to further event object information and the method further comprises using a display screen interface device to open the hypertext link to reveal further event object information on at least one successive display screen frameset.

30. The method of claim 26 wherein the stored event object is displayed as a hypertext link to further event object information and the method further comprises using a display screen

interface device to open the hypertext link to reveal further event object information on at least one succesive display screen frameset.

31. The method of claim 25 further comprising the step of filtering log data received according to one or more predetermined conditions so as to restrict the receipt of corresponding log data.

32. The method of claim 31 wherein the predetermined conditions are application name, host name, internal device alarm identifications, source address, destination address, destination port, and protocol.

33. The method of claim 25 further comprising the step of opening a electronic communications link to other users on the computer system.

34. The method of claim 33 further comprising the step of sending an electronic message over the communications link to other users regarding an intrusion alarm.